AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

151 SOUTH VILLAGE DRIVE
WASHINGTON TOWNSHIP, OHIO, 45459
INCLUDING ALL OUTBUILDINGS AND CURTILAGE

Case No. 3:18mj467

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A-1

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B-1

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*

SEE ATTACHMENT C-1

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

ANDREA R. KINZIG, SPECIAL AGENT FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/27/18

Judge's signature

City and state: DAYTON, OHIO

MICHAEL J. NEWMAN, U.S. MAGISTRATE JUDGE
Printed name and title

ATTACHMENT A-1

DESCRIPTION OF LOCATION TO BE SEARCHED

151 SOUTH VILLAGE DRIVE, WASHINGTON TOWNSHIP, OHIO, 45459 ("SUBJECT PREMISES") is a single family, two-story residence with brick surrounding the first story, white siding surrounding the second story, and blue shutters surrounding the windows. The street address numbers are black in color and affixed to a white sign next to the front door. There is a two-car attached garage on the south side of the residence. The SUBJECT PREMISES is located on the northeast corner of South Village Drive and Whittington Drive. The SUBJECT PREMISES includes all outbuildings, curtilage, and vehicles parked on the SUBJECT PREMISES.

ATTACHMENT B-1

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and attempted receipt of child pornography), 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession and attempted of child pornography), 2251(a) and (e) (production or attempted production of child pornography), 2422(b) (coercion and enticement), and 1470 (transfer of obscene materials to minors), including but not limited to the following:

Computers and Electronic Media

1. The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and computer media will be conducted in accordance with the affidavit submitted in support of this warrant.

2. Computer hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks); cellular telephones and tablets; and digital cameras and recording devices.

3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

5. Computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents, and materials referencing or relating to the above-described offenses. Such records, documents, or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form that such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data obtained through computer or Internet-based communications, including data in the form of electronic records, documents, and materials, including those used to facilitate interstate communications, including but not limited to telephone (including mobile telephone), tablets, and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer- related equipment, such as fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Computer and Internet Records and Physical Records

9. Any records related to the possession, attempted possession, receipt, attempted receipt, production, and attempted distribution of child pornography; coercion and enticement; and transfer of obscene materials to minors.

10. Any images or videos of child pornography.

11. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

12. Any Internet history indicative of searching for child pornography.

13. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed and/or traded.

14. Any Internet or cellular telephone communications (including email, social media, etc.) with minors.

15. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

16. Evidence of utilization of the account names jhsteach and bballcoach.

17. Evidence of utilization of the Chatstep.com website.

18. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.

19. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored, or maintained), books, diaries, and reference materials.

20. Records of address or identifying information for individuals using computers located at the SUBJECT PREMISES and any personal or business contacts or associates of his, (however and wherever written, stored, or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user IDs, eIDs (electronic ID numbers), and passwords.

21. Any books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of

any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

22. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

23. Lists of computer and Internet accounts, including user names and passwords.

24. Any information related to the use of aliases.

25. Documents and records regarding the ownership and/or possession of the items seized from the SUBJECT PREMISES.

26. Any records, documents, and billing records pertaining to accounts held with telephone, electronic, and Internet service providers.

Photographs of Search

27. During the course of the search, photographs of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items seized from the residence.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A) and coercion and enticement (in violation of 18 U.S.C. §2422). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.

2. Along with other agents and investigators of the FBI and Christiansburg (Virginia) Police Department, I am currently involved in an investigation of child pornography and child exploitation offenses committed by **MARC GREENBERG**. This Affidavit is submitted in support of Applications under Rule 41 of the Federal Rules of Criminal Procedure for search warrants for the following:

   a. The residential property located at 151 South Village Drive, Washington Township, Ohio, 45459 (hereinafter referred to as the "**SUBJECT PREMISES**" and more fully described in Attachment A-1 hereto);

   b. The person of **MARC GREENBERG** (as more fully described in Attachment A-2 hereto).

3. This Affidavit is submitted in support of Applications for search warrants for the **SUBJECT PREMISES,** the person of **MARC GREENBERG**, and the Computer and Electronic Media (as defined in Attachments B-1 and B-2) located at the **SUBJECT PREMISES** and on the person of **MARC GREENBERG**. The purpose of the Applications is to seize evidence of violations of the following:

   a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess or attempt to possess child pornography;

   b. 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to receive or attempt to receive child pornography through interstate commerce;

   c. 18 U.S.C. §§ 2251(a) and (e), which make it a crime to produce or attempt to produce child pornography;

d. 18 U.S.C. § 2422(b), which make it a crime to use a facility of interstate commerce to coerce and entice another individual to engage in illegal sexual activities or attempt to do so; and

e. 18 U.S.C. § 1470, which make it a crime to transfer obscene materials to minors.

4. The items to be searched for and seized are described more particularly in Attachments B-1 and B-2 hereto and incorporated by reference.

5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

6. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the **SUBJECT PREMISES**, the person of **MARC GREENBERG**, and the Computer and Electronic Media (as defined in Attachments B-1 and B-2) located at the **SUBJECT PREMISES** and on the person of **MARC GREENBERG**.

7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime, contraband, fruits of crime, or other items illegally possessed, property designed for use, intended for use, or used in committing a crime of violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), 2252A(a)(2) and (b)(1), 2251(a) and (e), 2422(b), and 1470 are present at the **SUBJECT PREMISES**, on the person of **MARC GREENBERG**, and on the Computer and Electronic Media (as defined in Attachments B-1 and B-2) located at the **SUBJECT PREMISES** and on the person of **MARC GREENBERG**.

PERTINENT FEDERAL CRIMINAL STATUTES

8. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.

9. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or

facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.

10. 18 U.S.C. § 2252(a)(2)(B) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.

11. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.

12. 18 U.S.C. §§ 2251(a) and (e) states that it is a violation for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, when he knew or had reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so.

13. 18 U.S.C. § 2422(b) states that is a violation for any person to use the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so.

a. For purposes of the statute, 18 U.S.C. §2427 states that the term "sexual activity for which any person can be charged with a criminal offense" includes the production of child pornography, as defined in section 2256(8).

14. 18 U.S.C. § 1470 states that it is a violation for any person to knowingly use the mail or any facility or means of interstate or foreign commerce to transfer obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years, or attempts to do so.

BACKGROUND INFORMATION

Definitions

15. The following definitions apply to this Affidavit and Attachments B-1 and B-2 to this Affidavit:

a. "**Child Pornography**" includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. "**Visual depictions**" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. "**Minor**" means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. "**Sexually explicit conduct**" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).

e. "**Internet Service Providers**" or "**ISPs**" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data,

called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

f. An "**Internet Protocol address**", also referred to as an "**IP address**", is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

g. A network "**server**," also referred to as a "**host**," is a computer system that has been designated to run a specific server application or applications and provide requested services to a "client" computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.

h. A "**client**" is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and retrieve web pages for display. E-mail clients (like Microsoft Outlook or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.

i. "**Domain Name**" refers to the common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically ".com" for commercial organizations, ".gov" for the governmental organizations, ".org" for organizations, and, ".edu" for educational organizations. Second level names will further identify the organization, for example "usdoj.gov" further identifies the United States

governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as "www.usdoj.gov," to its currently assigned IP address (*i.e.,* 149.101.1.32), to enable the follow of traffic across the Internet.

j. "**Log Files**" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

k. "**Hyperlink**" (often referred to simply as a "link") refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. "resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.

l. "**Website**" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

m. "**Uniform Resource Locator**" or "**Universal Resource Locator**" or "**URL**" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

n. A "**Smartphone**" is a mobile cellular telephone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded applications.

o. **Wi-Fi** is a technology that allows electronic devices to connect to a wireless LAN network. Devices that use Wi-Fi technology include personal computers, video game consoles, smartphones, digital cameras, tablets, and modern computers.

p. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Background on Computers and Child Pornography

16. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

17. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

18. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

19. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

20. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

21. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

22. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Chatstep.com Website

23. Chatstep.com in an online chatroom administered by a developer in Santa Clara, California. The website allows users to create and enter online chatrooms either anonymously or by using a nickname. The website also allows users to share images and files by pasting links to the files in the chat sessions.

24. Chatstep.com allows users to chat via three chat options. The first option is for users to create a chatroom and choose a name for the room. The link and password for the room can be shared with up to 50 other users via social media. The second option is to join a

private room created by a friend. The friend must send the link to the private chatroom. The third option is to access a public chatroom.

25. In November 2017, Chatstep.com introduced the ability for users to create accounts. Accounts are verified by Chatstep.com via an email message. Since November 2017, accounts are required in order to share images and links. Users can alternatively choose to use the site anonymously by choosing a nickname and joining a room.

26. When a user joins a chatroom, the person's name/nickname, IP address, room name, and time stamp are recorded and maintained in Chatstep.com's records. Chatstep.com does not maintain the contents of chat messages.

FACTS SUPPORTING PROBABLE CAUSE

27. In 2009, **MARC GREENBERG** was investigated by the FBI, New York Internet Crimes Against Children (ICAC) Task Force, and Naval Criminal Investigative Services (NCIC) for child pornography offenses. The investigation determined the following information:

a. From approximately January 2009 through April 2009, **MARC GREENBERG** utilized the America On Line (AOL) screen names of bballguy5555@aol.com and aig2010@aol.com to communicate with three separate undercover law enforcement officers who were posing as 12- and 13-year old girls on AOL. During this time period, **MARC GREENBERG** entered various AOL chatrooms that were geared toward meeting minor females and identified himself as an 18-year old male from Ohio; a 25-year old male from Indianapolis, Indiana; and a 31-year old male from Pennsylvania named "Justin". A series of sexually explicit conversations ensued between the undercover agents and **MARC GREENBERG**, during which **MARC GREENBERG** used his computer's web camera to stream live videos and pictures of his exposed penis and himself masturbating.

b. A federal search warrant was executed at **MARC GREENBERG's** residence on or around May 4, 2009. Various computer media belonging to **MARC GREENBERG** were seized pursuant to the warrant. A forensic analysis of the computer media revealed approximately 18 images containing child pornography.

28. On or around August 4, 2010, **MARC GREENBERG** pled guilty to one count of possession of child pornography, in violation of 18 U.S.C. §§2252(a)(4), and one count of transfer of obscene material to minors, in violation of 18 U.S.C. §1470. On or around November 5, 2010, **MARC GREENBERG** was sentenced to two years imprisonment and five years of supervised release. As part of his conviction, **MARC GREENBERG** is required to register as a sex offender for a period of 25 years.

29. In March 2018, the Christiansburg (Virginia) Police Department conducted an online investigation to identify individuals who were utilizing the Chatstep.com website to commit child exploitation offenses. On or around March 22, 2018, an undercover

investigator who will be referred to for purposes of this Affidavit as "UCO-1" logged onto the Chatstep.com website using a computer located in or around Christiansburg, Virginia. UCO-1 entered a public chatroom called "AFatherFigure".

30. While in the "AFatherFigure" chatroom, UCO-1 received a private message from a user who utilized the account name "bballcoach". In an exchange of messages in this chatroom, UCO-1 identified herself as being in the sixth grade in school. The "bballcoach" user indicated that he was a teacher and lived in Florida. The "bballcoach" user then asked to chat with UCO-1 in a private chatroom. UCO-1 agreed, and the "bballcoach" user provided UCO-1 with the name of a chatroom and password to access the room. Below is a transcript of this initial conversation in the "AFatherFigure" chatroom:

bballcoach:	hi. what grade you in?
UCO-1:	6th
bballcoach:	cool. i teach 7th. what are you up to today?
UCO-1:	cool snow day
bballcoach:	really? what part of the country you in?
UCO-1:	va u?
bballcoach:	florida. little better weather. you want to chat in private?
UCO-1:	oh nice ok
bballcoach:	i am in rm Sam41 pw 1234

31. Using the password provided by the "bballcoach" account user, UCO-1 entered a chatroom called "Sam41". In this chatroom, the "bballcoach" user utilized the account name of "jhsteach". Below is a summary of the communications in this chatroom:

a. UCO-1 identified that she was 11 years old, and the "jhsteach" account user identified that he was 22 years old.

b. The "jhsteach" account user sent UCO-1 two photographs: one that depicted an adult male wearing pants but no shirt and one that depicted an erect penis of an adult male. Based on my training and experience, I believe that the photograph depicting the erect penis constitutes obscene material.

c. On several occasions, the "jhsteach" account user requested photographs of UCO-1. Although the "jhsteach" account user did not specifically request nude photographs, the context of the messages indicated to me (based on my training and experience) that he wanted such photographs. The "jhsteach" account user also requested UCO-1 to remove all of her clothing and then asked if they could communicate via a web camera. Based on my training and experience, I believe that the requests made by the "jhsteach" account user for pictures of UCO-1, as well as his attempts to communicate with UCO-1 via web camera while she was purportedly nude, is consistent with someone attempting to obtain child pornography.

d. While UCO-1 was purportedly nude, the "jhsteach" account user instructed her to masturbate. The "jhsteach" account user also talked about the possibility of engaging in sexual intercourse with UCO-1.

e. Below are excerpts of the chat between the "jhsteach" account user and UCO-1 in the "Sam41" chatroom:

jhsteach:	so do you have plans for the rest of the day?
UCO-1:	not relly
UCO-1:	mom says to stay in apt
jhsteach:	so what do you like to do when you get bored?
UCO-1:	watch Netflix mainly lol
jhsteach:	that's sweet. probably better than what i do
UCO-1:	oh what u do?
jhsteach:	i usually masturbate
jhsteach:	would you like to see what i look like?
UCO-1:	oh lol
UCO-1:	yea totally
jhsteach:	*Sends photograph of adult male wearing pants but no shirt, standing in what appears to be a bathroom*
jhsteach:	noting special i know but hope you like
UCO-1:	whoa ur HOTTTTT
jhsteach:	awww. not really but thanks
jhsteach:	can i see one of you?
	. . . . .
UCO-1:	*Sends link to photograph of purported female child*
jhsteach:	wow. you are very pretty
UCO-1:	no u think
jhsteach:	yes. love yoru eyes and your smile. makes me want to see so much more of you. haha
	. . . . .
jhsteach:	bet you have a great body too. wish i could see you in a bikini
UCO-1:	idk i don't think so
jhsteach:	i understand, but i would show you anything you wanted.
jhsteach:	do you mind if i, um, masturbaet while we chat?
UCO-1:	um ok
UCO-1:	lol
UCO-1:	what u mean show me
jhsteach:	lik if you wanted to see more of me, i would let you.
UCO-1:	cool
jhsteach:	you ever seen boy naked?
UCO-1:	um on here I have lol
UCO-1:	not for real
jhsteach:	you like it?
UCO-1:	yea

jhsteach:	you ever show them anything?
UCO-1:	lol no
jhsteach:	you shy?
jhsteach:	you shouldnt be. you are super cute
UCO-1:	kinda
UCO-1:	yea
UCO-1:	ty u make me smile
jhsteach:	ty. you make me very hard
UCO-1:	lol no really
UCO-1:	u dont care im 11?
jhsteach:	want me to provie t?
UCO-1:	lol k
jhsteach:	*Sends photograph of the erect penis of what appears to be an adult male*
UCO-1:	wow :)
jhsteach:	you like it? Is it like the other men you have seen?
UCO-1:	um bigger i think
jhsteach:	haha. it would feel good in your mouth
	. . . . .
jhsteach:	can I see more of you?
UCO-1:	i cant
UCO-1:	i have to use my moms phone
	. . . . .
jhsteach:	take off your clothes please
UCO-1:	k
jhsteach:	you naked?
UCO-1:	yea
	. . . . .
jhsteach:	got a cam?
UCO-1:	no they turn them off
UCO-1:	i use school tab
jhsteach:	dang. do how do you feel sitting there naked?
	. . . . .
jhsteach:	k. open your legs for me courtney
UCO-1:	k
jhsteach:	now run yoru hand up and down your pussy
	. . . . .
jhsteach:	slide a finger into your hole
	. . . . .
jhsteach:	get your legs wide and slide a finger in
	. . . . .
jhsteach:	but wouldn't you want to lose yoru virginity to me?
UCO-1:	oh um why u wanna w me?
Jhsteach:	id love being yoru first

32. On or around March 22, 2018, UCO-1 served an administrative subpoena to Chatstep.com requesting IP addresses that were utilized to access the "Sam41" chatroom, as well as IP addresses utilized by the "bballcaoch" screen name – both for the approximate time period of February 22, 2018 through March 22, 2018. Records received from Chatstep.com in response to the subpoena provided the following information (among other information):

a. The "jhsteach" account user accessed the Sam41 chatroom on March 9, 2018 at approximately 18:11:35 UTC, utilizing the IP address of 2602:306:bd17:3580:fd4d:6237:73e2:9544.

b. The "bballcoach" account user accessed the "AFatherFigure" chatroom on March 22, 2018 at approximately 13:50:59 UTC, utilizing the IP address of 2602:306:bd17:3580:6c04:e9d6:3515:43a1.

33. AT&T was identified as the Internet Service Provider for the two IP addresses noted above. On or around March 30, 2018, UCO-1 served AT&T with administrative subpoenas requesting subscriber information for these two IP addresses on the two dates and times identified above. Records received in response to the subpoenas identified that both of the IP addresses were subscribed to an account in the name of **MARC GREENBERG**, with a service address of 690 East Whipp Road in Centerville, Ohio.

34. On or around May 21, 2018, an FBI investigator served Chatstep.com with an additional administrative subpoena requesting chatrooms entered and IP addresses utilized by the "bballcoach" and "jhsteach" account users. Records received from Chatstep.com in response to the subpoena provided the following information (among other information):

a. The "jhsteach" account was a registered account on Chatstep.com. The account was created on or around January 18, 2018. The email address bball3223@hotmail.com was utilized to verify the account.

b. The "bballcoach" account user was not a registered account on Chatstep.com. Therefore, the account user had the ability to use the site anonymously.

c. The "jhsteach" account user entered chatrooms on approximately 347 occasions during the approximate time period of November 22, 2017 through May 24, 2018. I have reviewed the names of these chatrooms, and based on my training and experience, some of the names appear to be consistent with chatrooms utilized by teenagers. Examples of these chatrooms include Almost18, BarelyLegal, CastingSchoolSLuuts, HighSchoolBoredF, HSFemms, SchoolGals, and StudentBJ's.

d. The "bballcoach" account user entered chatrooms on approximately 143 occasions during the approximate time period of November 4, 2016 through October 23, 2017. I have reviewed the names of these chatrooms, and based on my training and experience, some of the names appear to be consistent with

chatrooms utilized by teenagers. Examples of these chatrooms include HSAthleeetes, HSBoredF, preteenlotizards, and SeniorsHS.

e. The logs of IP addresses utilized by the "jhsteach" account user included the following:

i. During the approximate time period of November 22, 2017 through April 22, 2018, a number of which appear to be dynamic and static IP addresses serviced by AT&T were primarily utilized by the account user. The suspected static IP addresses of 107.209.115.88 was utilized on approximately 61 occasions.

ii. During the approximately time period of April 23, 2018 through May 24, 2018, a number of which appear to be dynamic and static IP addresses serviced by both AT&T and Charter Communications were utilized by the account user.

f. The logs of IP addresses utilized by the "bballcaoch" account user included the following:

i. During the approximate time period of November 4, 2016 through October 23, 2017, a number of what appear to be dynamic and static IP addresses serviced by AT&T were primarily utilized by the account user. The suspected static IP addresses of 107.209.115.88 (the same IP address utilized to access the "jhsteach" account on approximately 61 occasions, as detailed above) was utilized on approximately 77 occasions.

35. On or around May 25, 2018, an FBI investigator served an administrative subpoena to AT&T requesting subscriber information for a sample of six of the IP addresses utilized by the "jhsteach" and "bballcoach" accounts – including the IP address of 107.209.115.88 (which was utilized to access the "jhsteach" account on approximately 61 occasions and the "bballcoach" account on approximately 77 occasion). Records received in response to the subpoena identified that each of these IP addresses was subscribed to an account in the name of **MARC GREENBERG**, with a service address of 690 East Whipp Road in Centerville, Ohio.

36. On or around May 25, 2018, an FBI investigator served an administrative subpoena to Charter Communications requesting subscriber information for a sample of two of the IP addresses utilized by the "jhsteach" account. Records received in response to the subpoena identified that both of these IP addresses were subscribed to an account in the name of **MARC GREENBERG**, with a service address of the **SUBJECT PREMISES**. The records indicate that the account was activated on or around April 23, 2018.

37. Records from the Montgomery County (Ohio) Sheriff's Office identified that **MARC GREENBERG** has been compliant in registering his address as required by his sex offender registration requirements. The records identified that during the approximate

time period of February 9, 2013 through May 16, 2018, **MARC GREENBERG** reported that his address was 690 East Whipp Road in Centerville, Ohio. The records further identified that on or around May 16, 2018, **MARC GREENBERG** reported that he had moved to the **SUBJECT PREMISES**. A detective of the Montgomery County Sheriff's Office went to the **SUBJECT PREMISES** on or around May 16, 2018, to verify the new address. The detective's notes documented that he personally contacted **MARC GREENBERG** at the residence, and that **MARC GREENBERG** identified that he was in the process of moving into the residence.

38. Records from the Montgomery County (Ohio) Auditor's website identified that the residence located at 690 East Whipp Road in Centerville, Ohio, was previously owned by MARIBETH GREENBERG. The records identified that MARIBETH GREENBERG sold the residence to a third party on or around May 29, 2018. The investigation has determined that MARIBETH GREENBERG is **MARC GREENBERG**'s wife.

39. Records from the Montgomery County (Ohio) Auditor's website also identified that the **SUBJECT PREMISES** is currently owned by **MARC GREENBERG** and MARIBETH GREENBERG. The records identified that **MARC GREENBERG** and MARIBETH GREENBERG purchased the property on or around December 21, 2017.

40. On or around June 14, 2018, I drove by the **SUBJECT PREMISES**. I observed a vehicle registered to MARIBETH GREENBERG parked in the driveway of the residence. In his sex offender registration paperwork, **MARC GREENBERG** has identified that he drives this vehicle. I also observed an adult male who appeared to be **MARC GREENBERG** in the side yard of the residence.

41. As detailed above, the "jhsteach" account user sent UCO-1 a photograph of an adult male standing in a bathroom. The adult male depicted in the photograph does not appear to be **MARC GREENBERG**. Also as detailed above, the "bballcoach" and "jhsteach" account user identified that he was a 22-year old man who lived in Florida. Based on my training and experience, I know the following information:

a. Individuals involved in child exploitation offenses often utilize one or more aliases as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. The previous investigation of **MARC GREENBERG** conducted in 2009 identified that he utilized at least three aliases (as detailed above).

b. It is not uncommon for offenders to utilize fictitious photographs when exchanging photographs with victims or other offenders. In my experience, individuals utilize fictitious photographs to conceal their identities and/or to enhance their appearance (i.e., in an effort to make themselves more attractive to victims).

42. Based on all of the information detailed above, I believe that **MARC GREENBERG** is the user of the "jhsteach" and "bballcoach" accounts on the Chatstep.com website. I also believe that he has utilized these accounts to send obscene material to one or more purported or actual minors and to solicit one or more purported or actual minors to produce and send him child pornography.

43. Also based on all of the information detailed above, it is reasonable to believe that:

a. **MARC GREENBERG** previously lived at and utilized one or more computer devices at 690 East Whipp Road in Centerville, Ohio.

b. For a period of time, including at least April 2018 through May 2018, **MARC GREENBERG** had access to both the residence at 690 East Whipp in Centerville, Ohio and the **SUBJECT PREMISES**, and he utilized one or more computer devices at both residences.

c. Beginning on a date unknown, but at least by May 29, 2018, and continuing through the present, **MARC GREENBERG** has exclusively lived at and utilized one or more computer devices at the **SUBJECT PREMISES**.

44. Based on my training and experience, I know that it is not uncommon for individuals involved in child pornography offenses to utilize multiple computer devices in furtherance of their child pornography and child exploitation activities. Individuals sometimes save their files to multiple devices to allow easy access to the files and/or to back-up the devices in case of a computer failure.

45. Again based on my training and experience, I know that collectors of child pornography often use external devices (such as thumb drives, external hard drives, CD's/DVD's, SD cards, SIM cards, etc.) to store child pornography. The accumulation of child pornography files may fill up the space on the hard drives of computers, and external devices are needed to store and maintain files. These devices also serve as a mechanism for transferring files from one computer to another. In my experience, individuals maintain such external devices in their residences. Given their portable size, individuals sometimes maintain the devices on their persons and/or take the devices with them when they travel by vehicle.

46. Based on my training and experience, I know that individuals are increasingly utilizing laptop computers and other smaller devices such as cellular telephones, iPads, and tablets to do their computing. These devices are typically maintained in the owners' residences. Due to their portable nature, individuals also sometimes maintain the devices on their persons and/or take the devices with them when they travel by vehicle.

47. Based on my training and experience, I know that collectors of child pornography often maintain their collections for long periods of time. In addition, computer evidence typically persists for long periods of time, and computer data can often be recovered from deleted space (as further detailed above).

48. Based on my training and experience, individuals involved in child exploitation schemes often utilize social media accounts, email addresses, messenger applications, and dating websites as a means to locate and recruit victims. They then use the chat functions on these websites, as well as email accounts and other messenger applications, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

49. Also based on my training and experience, I know that individuals involved in child exploitation offenses utilize a variety of threats and manipulation techniques to compel their victims to engage or continue engaging in the illicit sexual activities (including the production of child pornography). These threats and manipulations are intended to control the victims and their activities, prevent them from stopping the activities, and prevent them from contacting law enforcement officers. It is common for such offenders to threaten that if the victims end the illicit sexual activities, the offenders will harm the victims and their family members and / or bring notoriety and shame to the victims by exposing the victims' involvement in the sexually explicit conduct.

50. In my experience, individuals involved in child exploitation schemes often communicate with others involved in similar offenses via e-mail, social media, and other online chatrooms. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.

51. In my experience, individuals often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, and on Internet bulletin boards; Internet P2P file sharing programs; Internet websites; and other sources. Evidence of multiple aliases, accounts, and sources of child pornography can often be found in the subjects' email communications. Evidence of the multiple aliases, accounts, and sources of child pornography are often found on the computer devices located at the offenders' residences, in their vehicles, and on their persons.

52. I know, in my experience, that individuals involved in child exploitation offenses sometimes print the pictures in hard copy format. Such individuals do so both for easier access / viewing of the files and to back-up the files in the event that one computer device becomes damaged and broken. Similarly, these individuals often save contact information (i.e., email addresses and account names) for those with whom they communicate about child exploitation offenses in multiple locations.

//

//

53. In addition, individuals often maintain lists of their electronic accounts (including associated user names and passwords) and their aliases in handwritten format. These papers are sometimes maintained in close proximity to their computers for easy access. In other cases, the papers may be hidden or maintained in secure locations to avoid detection by others.

54. In my experience, I know that many cellular telephones, iPads, and tablets store information related to IP addresses and Wi-Fi accounts that the telephone accessed and GPS data. This information helps in identifying the subjects' whereabouts during the criminal activities and the travels they took to get to these locations.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

55. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

56. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or

interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

57. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA

58. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. On-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. Examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

e. Surveying various file directories and the individual files they contain;

f. Opening files in order to determine their contents;

g. Scanning storage areas;

h. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachments B-1 and B-2; and

i. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachments B-1 and B-2.

CONCLUSION

59. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime, contraband, fruits of crime, or other items illegally possessed, property designed for use, intended for use, or used in committing a crime of violations of federal law, may be located at the **SUBJECT PREMISES,** on the person of **MARC GREENBERG**, and on the Computer and Electronic Media (as defined in Attachments B-1 and B-2) located at the **SUBJECT PREMISES** and on the person of **MARC GREENBERG**: 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), 2252A(a)(2) and (b)(1), 2251(a) and (e), 2422(b), and 1470.

60. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 and B-2.

Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 27th of June 2018

MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE